DP-307767

VEHICLE DISABLE SYSTEM

Technical Field

[0001] The present invention generally relates to security systems and more particularly relates to systems for disabling the movement of a vehicle.

Background of the Invention

[0002] Existing vehicle security systems are primarily antonymous systems used to detect theft or vandalization of a vehicle, vehicle components, or unauthorized vehicle entry. More sophisticated vehicle security systems exist that provide some form of vehicle status information which is relayed back to a monitoring center. The OnStar® provides the ability for the vehicle operator to electronically communicate by way of "voice communications" with someone manning a monitoring center. These communications are typically used to verbally provide routing, and other navigational information to the vehicle operator. They are also used by the vehicle operator to communicate vehicle operational problems to call center so that the appropriate assistance can be dispatched to the vehicle operator.

[0003] In view of the recent homeland security issues, protecting vehicles against theft or vandalism has become secondary, giving way to a primary concern of protecting citizens from vehicles that could possibly used for mass destruction of property or human life. The present invention is particularly well suited to remotely disable any vehicle in a controlled manner thereby allowing the vehicle operator, at all times, maintain control of the vehicle.

Brief Description of the Drawings

[0004] Figure 1 is a diagrammatic depiction of the various communication links and methods used by the disable system of the present invention to communicate with, and to disable, a vehicle.

[0005] Figure 2 is a diagrammatic view of the hardware used to implement the preferred of the disclosed vehicle disable system.

Detailed Description of the Preferred Embodiment

[0006] Now referring to Figures 1 and 2, the vehicle disable system 10 of the present invention is preferably integrated with onboard computer 12 of vehicle 14. Although the present invention will be primarily discussed as it applies to heavy duty truck vehicles, there is nothing that prohibits using the present invention on any type of vehicle, including automobiles and aquatic based vehicles. Modern trucks typically employ an onboard computer 12 to manage a whole host of vehicle operations. Onboard computer 12 is typically mounted under the dash of vehicle 14; however, it can also be mounted in other locations within the vehicle passenger compartment as well as in the engine compartment. Onboard computer 12 is used to carry out the logic methodology (herein set forth in detail below) associated with disabling the vehicle in a controlled manner. Although the preferred embodiment of the present invention is to implement the truck disable system 10 by way of a digital, onboard computer 12, it is to be understood that disable system 10 can also be implemented, equally as well, using discrete digital logic and/or well known analog electronic circuit components. It is also contemplated that the truck disable system 10 of present invention is equally suited for both original equipment manufacture and as an after market unit (sold for installation on existing vehicles).

[0007] Wireless modem 16 provides the communication link between onboard computer 12 and control center 18. The communication format between control center 18 on onboard computer 12 can take place in any number of formats such as Plain Old Telephone Service (POTS), or, by way of, an internet link.

Security Modes

[0008] The following describes four preferred security modes in which vehicle disable system 10 can be operated. All of these four modes include disabling vehicle 14 in a secure, controlled manner thereby preventing unauthorized movement of the vehicle. In cases where vehicle 14 is transporting dangerous substances, vehicle disable system 10 will eliminate, or substantially impede, any attempts to steal or misuse the vehicle.

Reported Theft Security Mode

[0009] In this scenario, the vehicle driver reports the theft of vehicle 14 to call center 18. This method of communication between the vehicle operator and call center 18 would, in most instances, take place over a conventional telephone communication link 20. Thereafter, call center 18 communicates with vehicle 14 using POTS or, the IP address assigned to onboard computer 12. When the internet is used as the means of effecting communication between control center 18 and vehicle 14, conventional password technology can be used to secure the integrity of the internet communications session.

[0010] Onboard computer 12 includes an internet connection module, a web server secured access module, and a web page provider module. These three modules in conjunction with wireless modem 16 enable onboard computer 12 to communicate with command center 18 by way of the internet. Upon receipt of a correct password from control center 18, serves a webpage to call center 18 by way of the web page provider module 13. The served web page gives various system options to call center 18 operators, one of which is the shutdown option. If call center 18 operators select the shutdown option, onboard computer 12 requests confirmation form call center 18 by requesting a vehicle shutdown password. Upon receiving a valid password, onboard computer 12 initiates a shutdown sequence. This shutdown sequence includes, amongst other things, disabling the throttle position sensor signal received by engine control computer 26 on signal input line 28. This interruption can take place using any number of techniques, such as by using computer 12 to place a voltage reference signal on line 30 which is equivalent to an engine idle reference signal. Once this "engine idle" voltage reference is placed on line 30, computer 12 activates relay 32 by way of control line 32 thereby removing from line 28 the signal present from line 24 and replacing it with the signal from line 30. This causes engine control computer 26 to receive an engine idle command thereby causing the engine to enter into an idle mode. Thus, the present invention is effective for essentially eliminating throttle position sensor 22 from the circuit causing the engine to "think" that the driver is not depressing the accelerator pedal. By disabling the vehicle in this manner, engine power is still made available for enabling power steering and power braking assist functions. It is critical that these power assist functions stay intact

during a controlled shutdown operation so that if the vehicle is moving, the vehicle operator can maneuver the vehicle to a safe location.

[0011] Relay 34 is shown in Figure 2 in a deenergized state. In this deenergized state, engine throttle position sensor 22 communicates directly with engine control computer 26 via lines 24, and 28. In an alternative embodiment, relay 34, when deenergized, can be placed in a state whereby line 28 is electrically connected to line 30. This has the distinct advantage that before the vehicle engine 19 can be taken out of an idle mode, onboard computer 12 must be active (in order to activate relay 34 by way of line 32). It is also contemplated in the present invention that relay 34 can be integrated into the housing of throttle position sensor 22. This integration may have both cost and security advantages. Although lines 24, 28, 30 and 32 are in their simplest embodiment, simple, single conductors, it is anticipated that digital bus communication can be used to communicate between computer 12 and relay 34. This digital data interface could be implemented in any number of well know formats including pulse width modulation, or serial data interface (such as RS-232, J1587, J1939, etc.). When onboard computer 12 is commanded (via control center 18) to disable vehicle 14, it applies a voltage to the relay (by way of line 32) causing line 28 to be disconnected from line 24 and to be connected to line 30. As was mentioned above, the voltage provided on line 30 is such that the engine control computer 26 understands that it is now being commanded to put the engine in an idle condition.

Route Tracking Security Mode

[0012] Tracking vehicle 14 using periodic GPS (Global Positioning System) by way of a wireless internet connection is possible by virtue of using well known global position sensor technology. Specifically, an onboard global positioning system 21 can be used to receive GPS signals and translate those signals into vehicle position information which is sent to control center 18 via wireless modem 16. It is contemplated that the control center can compare the received GPS signals with preprogrammed route information. If vehicle 14 deviates from the preprogrammed route by more than a predetermined distance, control center 18 can initiate communications with the vehicle operator asking him to input a password in order to

permit continued operation of the vehicle. If the password is not entered, or is entered incorrectly, control center 18 can initiate vehicle shutdown as discussed above.

Periodic Driver Authentication Security Mode

[0013] Under this methodology, driver authentication is conducted either periodically or every ignition cycle (every time the vehicle engine 19 starts), by forcing the driver to enter an identification number. A technique of required periodic entry of an ID number guarantees that the driver is authorized even when remote communications are not possible between onboard computer 12 and command center 18. Such communications might not be possible when adverse whether conditions prohibit telecommunications between wireless modem 16 and control center 18. The periodic entry of the driver ID ensures that the driver is the driver authorized to operate the vehicle. This ID can be either fixed, changed periodically by control center 18, or changed automatically by some other means based on a shared "rolling code" algorithm. The implementation of a "rolling code" algorithm requires the truck driver to have a means for obtaining new IDs as a function of time /date (e.g., a secure ID). This ID would be a function of time, date and the vehicle ID.

[0014] Where the function is a standard crypto-rolling code, the ID can be entered either by way of a keyboard 27 connected directly to onboard computer 12 or by way of voice input processed by a voice recognition module 23. ID input by way of voice communication is the preferred mode of data input by the vehicle driver because it promotes greater levels of safety by allowing the vehicle operator to communicate with computer 12 while still keeping his "eyes on the road." In normal situations, when there is a low level security alert status, computer 12 may only require driver ID verification every two to four hours or so. This infrequent ID request will have minimal impact on the driver's normal driving routine; however, in times when the nation is put on high alert status, control center 18 can require more frequent verification of driver ID (perhaps as frequently as every 15 minutes or so). This increased level of driver inconvenience is offset by the need of greater diligence during times of "high alert" status. The internet connectivity of computer 12 permits this level of dynamic behavior.

Alarm Security Mode

[0015] In the event of a hijack attempt, the truck driver can press an alarm button on a keyboard connected to computer 12 or manually activate a panic button on a remote key FOB transmitter 25. A remote transmitter could also be used to immediately enable the security features of vehicle 14 thereby requiring reentry of the driver ID before the vehicle could be operated. In the alarm security mode, control center 18 would be immediately notified via the wireless modem link that a problem as occurred.